

## Claims

- [c1] 1. A system for globally restricting client access to a secured web site comprising:  
a first web server configured to:  
receive a client login; and  
return a cookie to the client containing an access credential wherein the access credential contains at least one role-based attribute specific to the client; and  
a second web server hosting a secured web site having an associated security expression wherein the security expression contains at least one role-based access privilege for the web site, the second web server configured to:  
receive the cookie containing the access credential in response to an HTTP request from the client; and  
if the access credential contains a role-based attribute in common with the security expression, grant the client access to the secured web site.
- [c2] 2. The system of claim 1 wherein the access credential and security expression additionally contain a token attribute for locally defined access to the secured web site.
- [c3] 3. The system of claim 2 wherein the token attribute contains permission re-granting capability.
- [c4] 4. The system of claim 1 wherein the access credential is digitally signed.
- [c5] 5. The system of claim 1 wherein role based attributes are assigned to the client based on the client's login password.
- [c6] 6. The system of claim 5 wherein the first web server is additionally configured to synchronize client passwords among more than one password repository.
- [c7] 7. The system of claim 1 wherein the web site contains a web-based application.

- [c8] 8.The system of claim 1 wherein the access credential expires after a predefined period of time.
- [c9] 9.The system of claim 1 wherein the access credential is encoded.
- [c10] 10.A method for globally restricting client access to a secured web site comprising:  
receiving a client login at a first web server;  
returning a cookie to the client containing an access credential wherein the access credential contains at least one role-based attribute specific to the client;  
receiving the cookie containing the access credential from the client in response to an HTTP request at a second web server wherein the second web server hosts a secured web site having an associated security expression containing at least one role-based access privilege; and  
if the access credential contains a role-based attribute in common with the security expression, granting the client access to the secured web site.
- [c11] 11.The method of claim 10 wherein the access credential and security expression additionally contain a token attribute for locally defined access to the secured web site.
- [c12] 12.The method of claim 11 wherein the token attribute contains permission re-granting capability.
- [c13] 13.The method of claim 10 wherein the access credential is digitally signed.
- [c14] 14.The method of claim 10 wherein role based attributes are assigned to the client based on the client's login password.
- [c15] 15.The system of claim 14 wherein the first web server is configured to synchronize client passwords among more than one password repository.
- [c16] 16.The system of claim 10 wherein the web site contains a web-based application.

[c17] 17.The system of claim 10 wherein the access credential expires after a predefined period of time.

[c18] 18.The system of claim 10 wherein the access credential is encoded.

17. The system of claim 10 wherein the access credential expires after a predefined period of time.

18. The system of claim 10 wherein the access credential is encoded.